CLAIMS

1. A content distribution system comprising:

a data processing apparatus of a user for receiving a content supplied from a content transmitter;

a data processing apparatus of a third party trusted by both the content transmitter and the user; and

a communications network connecting the data processing apparatuses of the user and the third party for mutual data communication;

wherein the data processing apparatus of the user is provided with a tamper-resistant device storing data inaccessible from outside;

wherein the data processing apparatus of the third party transmits first data to the data processing apparatus of the user, the first data relating to an encryption key that decodes a cipher generated by the content transmitter, the encryption key being obtained only within the tamper-resistant device; and

wherein the tamper-resistant device decodes the cipher by using the first data from the data processing apparatus of the third party.

2. A content distribution system comprising:

a data processing apparatus of a content transmitter that transmits a content;

a data processing apparatus of a user that receives the content;

a data processing apparatus of a third party trusted by both the content transmitter and the user; and

a communications network connecting the data processing apparatuses of the content transmitter, the user and the third party for mutual data communication;

wherein the data processing apparatus of the content transmitter supplies a cipher to the data processing apparatus of the user;

wherein the data processing apparatus of the user is provided with a tamper-resistant device storing data inaccessible from outside;

wherein the data processing apparatus of the third party transmits first data to the data processing apparatus of the user, the first data relating to an encryption key that decodes the cipher, the encryption key being obtained only within the tamper-resistant device; and

wherein the tamper-resistant device decodes the cipher by using the first data from the data processing apparatus of the third party.

3. The system according to claim 2, wherein the data processing apparatus of the third party stores a public key and a secret key, the public key being transmitted to the data processing apparatus of the content transmitter as required by the data processing apparatus of the content transmitter;

wherein the data processing apparatus of the content transmitter encodes the encryption key by using the public key from the data processing apparatus of the third party, the encoded encryption key being transmitted to the data processing apparatus of the user;

wherein the data processing apparatus of the user causes the tamper-resistant device to generate second data based on the encoded encryption key from the data processing apparatus of the content transmitter, the second data being transmitted to the data processing apparatus of the third party; and

wherein the data processing apparatus of the third party generates the first data based on the secret key and the second data supplied from the data processing apparatus of the user.

4. The system according to claim 3, further comprising an additional third party, wherein the tamper-resistant device divides the second data into pieces one of which is received by a relevant one of the third parties.

5. The system according to claim 3, wherein the tamper-resistant device allows mixing of a random number component in generating the second data based on the encoded encryption key, while also allowing removal of the random number component from the first data in decoding the cipher by using the first data.

6. The system according to claim 2, wherein the tamper-resistant device stores information on the public key in a form of a digital certificate by an authentication agency, the tamper-resistant device being supplied to the user after the user is identified by the authentication agency; and

wherein the data processing apparatus of the third party confirms the identification of the user based on the public key information supplied in the form of the digital certificate from the data processing apparatus of the user.

7. A tamper-resistant device used in a content distribution system, the system comprising a data processing apparatus of a content transmitter to supply an encrypted content, a data processing apparatus of a user to receive the supplied content, a data processing apparatus of a third party which is trusted by both the content transmitter and the user and supplies data on a key to decode the encrypted content, and a communications network connecting the respective data processing apparatuses to each other for mutual data communication, the tamper-resistant device comprising:

a memory storing data inaccessible from outside;

a key obtainer that restores the decoding key based on the key data supplied from the data processing apparatus of the third party; and

a decoder that decodes the encrypted content by using the decoding key restored by the key obtainer.

8. A server used in a content distribution system, the system comprising a data processing apparatus of a content transmitter to supply an encrypted content, a data processing apparatus of a user to receive the supplied content, a data processing apparatus of a third party trusted by both the content transmitter and the user, a communications network connecting the respective data processing apparatuses to each other for mutual data communication, and a tamper-resistant device provided on the data processing apparatus of the user for storing data inaccessible from outside, the server working as the data processing apparatus of the third party, the server comprising:

a data generator that generates first data relating to a key to decode the encrypted content from the data processing apparatus of the content transmitter, the decoding key being generated only within the tamper-resistant device; and

a data transmitter that sends the first data to the data processing apparatus of the user via the communications network.

9. A computer program used in a content distribution system, the system comprising a data processing apparatus of a content transmitter to supply an encrypted content, a data processing apparatus of a user to receive the supplied content, a data processing apparatus of a third party trusted by both the content transmitter and the user, a communications network connecting the data processing apparatuses of the content transmitter, the user and the third party for mutual data communication, and a tamper-resistant device provided on the data processing apparatus of the user, the tamper-resistant device storing data inaccessible from outside, the computer program being prepared for controlling the data processing apparatus of the third party, the computer program comprising:

a data generation program for generating first data relating to a key that decodes the encrypted content from the data processing apparatus of the content transmitter, the decoding key being generated only within the tamper-resistant device; and

a data transmission program for sending the first data to the data processing apparatus of the user via the communication network.

10. A content distribution process performed in a system that comprises a data processing apparatus of a user to receive an encrypted content supplied from a content transmitter, a data processing apparatus of a third party trusted by both the content transmitter and the user, and a communications network connecting the data processing apparatuses of the user and the third party for mutual data communication, the content distribution process comprising the steps of:

causing the data processing apparatus of the user to issue an instruction to the data processing apparatus of the third party for carrying out a procedure to make a payment for the content;

causing the data processing apparatus of the third party to send first data to the data processing apparatus of the user when the payment for the content is made from an account of the user to an account of the third party, the first data serving to provides a key that decodes the encrypted content, the decoding key being available only within the data processing apparatus of the user; and

causing the data processing apparatus of the user to decode the encrypted content using the first data supplied from the data processing apparatus of the third party.

11. The process according to claim 10, wherein the data processing apparatus of the user is provided with a tamper-resistant device that stores data inaccessible from outside, the decoding of the encrypted content being performed by the tamper-resistant device.

12. The process according to claim 10, wherein the data processing apparatus of the third party stores a public key and a secret key,

wherein the data processing apparatus of the user generates second data based on the decoding key, the decoding key being supplied from the content transmitter and encrypted by the public key, the second data being transmitted to the data processing apparatus of the third party, and

wherein the data processing apparatus of the third party generates the first data based on the second data and the secret key.

13. The process according to claim 12, wherein the data processing apparatus of the user allows mixing of a random number component in generating the second data based on the encrypted decoding key, the random number component being removed from the first data when the first data decodes the encrypted content.

14. The process according to claim 13, wherein the tamper-resistant device generates the second data and decodes the encrypted content.

15. The process according to claim 10, wherein the data processing apparatus of the third party carries out the payment procedure from the account of the third party to the account of the content transmitter when the data processing apparatus of the third party receives content confirmation notice from the data processing apparatus of the user.